The Emerging AI Policy for e-commerce Industry

Zehra Ozge Yildiz
Department of Informatics University of Sussex
Brighton, United Kingdom
yildiz.ozge@outlook.com

Dr Natalia Beloff
Department of Informatics University of Sussex
Brighton, United Kingdom
N.Beloff@sussex.ac.uk

ABSTRACT

For the fast-growing e-Commerce industry, the AI is the game-changer but is it really utilised in a most effective way or is it just a risky 'artificial balloon'? Is it gambling to rely on AI technologies without forming a dedicated policy? To answer these questions and propose a cautious approach towards the emerging technologies, in this explanatory research, the risks related to the fast adaptation of AI technologies addressed with recommended actions. Within the scope of the research, e-Commerce industry is analysed to reveal the issues related to AI implementations. Accordingly, the challenges of AI technologies have been questioned so that necessary precaution, preparation, and considerations can be pointed out. Accordingly, an AI policy for e-Commerce industry is formed for the businesses to benefit from the most recent technologies without risking the possible issues. Three main policy subjects have been determined as transparency of the technologies, accountability for the purpose, process and performance of them, and lastly, emerging user privacy and security related issues. For each policy subject, a review of the AI implementations, recent critics and forecasted expectations are investigated to list the recommendations for the candidate AI implementer. The research aims to provide an AI policy guideline for e-Commerce industry with a detailed overview of the outstanding issues, best practices and recommendations from scholars.

CCS Concepts

• Information systems→Information systems applications

Keywords

AI policy; Aigital information management; e- Commerce; New AI technologies; Transparency in AI; Accountability in AI; User trust in AI

1. INTRODUCTION

In the paper, the risks of AI technologies in e-Commerce industry have been addressed with an AI policy. Considering this aim, firstly, the need for a policy is pointed out through examining industry implementations, critics, future trends and upcoming legal enforcements. Later, the most important issues and risks are investigated under three main parts; **transparency**, **accountability**, and **user privacy**

ICIIT 2020, February 19–22, 2020, Hanoi, Viet Nam

ACM ISBN 978-1-4503-7659-4/19/07…$15.00
DOI: https://doi.org/10.1145/3385209.3385210

To sustain transparency, it is recommended for the e- Commerce companies to focus on communicating the reasoning behind the use of an AI technology with the end user. The end user is defined as the employees, managers and other users inside the company. To sustain transparency, it is advised to provide information about the process flow behind the mechanism of the technology to clarify how it works. Lastly, to sustain complete transparency, it is mentioned that the end user should be able to evaluate the outcome that is expected to obtain with the use the technology. Overall, the **purpose**, **process**, and **performance** (3Ps) are determined important to apply transparency while adapting AI technologies.

As a second policy, defining **accountability** is claimed to be a necessary part of an AI policy. Under this section, the need for addressing the ownership and responsibility of the technology for its outcome and performance have been investigated. As a recommendation, it is mentioned that both the legal and technical expert consultancy is needed while forming the AI policy.

Along with the transparency and accountability, the **security** and **user privacy**-related issues are addressed within the proposed AI policy. Paying attention to the industry practices and emerging needs, designing secure and easily accessible technologies are advised. While sustaining the security, the companies are also recommended to provide an easy access and control ability about the collected information and the mechanism behind the technology.

1.1 Methodology

An exploratory research methodology has been used to understand the risks related to AI technologies, uncover trends, and motivations in the e-Commerce industry to adopt them. By combining the literature review and case study research, the need for an AI policy and its proposed structure have been formed. Based on open-ended questions, the insights from the research have been provided as recommendations for an AI policy.

The underlying aim of the study is to develop ideas, hypotheses and a proposed structure for an AI policy based on real-life implementations, recommendations, and discussion among scholars. The findings can be beneficial for both potential adopters, policy makers and scientists of AI technologies in the e-Commerce industry.

2. THE EMERGING AI POLICY FOR THE E-COMMERCE INDUSTRY

2.1 What is an AI Policy

While the AI technologies promise great opportunities for the businesses, in terms of gaining a **sustainable competitive advantage** and **superior performance**, there is an anticipated **risk** about adopting the technologies without any pre-determined policy. Especially, for the fast-growing e-Commerce industry, the AI is the game-changer but is it utilised in a most effective way or is it just a fancy 'artificial balloon'? To answer this question and propose a different perspective towards the

emerging technologies, in this explanatory research, common AI challenges and implementations have been investigated. By combining **managerial** and **technical** knowledge on this topic, an AI policy framework for the e-Commerce industry has been studied.

The forward-thinking innovators like Elon Musk, Stephen Hawking, and Stuart Russell pointed out the importance of regulated AI research to avoid its risks [13]. The proclaimed risks vary from the risk to the existence of human civilization to the immorality of the AI systems. The question is that what kind of precautions must be considered today to avoid the risks of new AI technologies. It is also important to explore how the e-Commerce industry, as being one of the most likely industry for AI implementations, should prepare itself for the future.

The e-Commerce industry is using AI heavily as it enables abundant and profitable **predictions** [1]. Although there is an excessive expected gain for the implementation of the AI technologies to automate, fasten or improve business processes in e-Commerce, the companies should not rush and create an illusion out of it. According to the recent survey that is conducted for 3,000 business executives, managers and analysts from all around the world, three-quarters of the executives see AI as an opportunity to move into new businesses. Also, 85% believe AI will bring competitive advantage. On the other hand, when the execution analysed, only one in five companies has implemented AI in some of their business processes, and only one in twenty companies have performed AI in their business processes in a broad way.

When their AI strategy is analysed, less than 39% of all companies could provide a prepared plan [16], [10]. However, according to Ng [14], like many S&P 500 companies which were late to develop their internet strategy, in several years, companies which are not establishing an AI strategy today might regret and fall **behind** their competitors. In parallel to this claim, leading technology companies are competing to discover new application areas for AI technologies.

According to these findings, it can be claimed that a **strategical fit**, **change management** for the implementation, and an **AI policy** for the integration of business processes need further attention. The reason is that not only the technology firms but also, from governments to different industries, almost every organization is affected by these emerging technologies. Especially, with the changes in business processes, new business models, leadership styles and policies needed to guide the transition and increase productivity and efficiency. Each industry will benefit from AI differently and therefore, different strategical plans, procedures, and processes will be needed to benefit from these technologies most efficiently and effectively.

However, because of the limited scope of the research, close attention will be given to the e-commerce industry, its dynamics, and an AI policy framework for the companies.

It had been claimed that there will be a cultural shift for companies to adopt a more responsive approach to data protection. It is mentioned that in the future, auditors, who have access to the code, can be used to make the transparency an **obligation** rather than a 'nice to have' feature [15]. In parallel to this prediction, the responsive approach is already happening mandatorily rather than a voluntary action because there are countries like Germany, Argentina, and Japan, which forced Google to reveal specific search results that mislead users. Moreover, as of 2018, the European Union's General Data Protection Regulations gives individuals a right to an explanation for decisions made by AI implementations and other algorithms [9]. When the recent announcements reviewed, while a new AI policy package is released in April 2019 in Japan, EU states have declared their plans for cooperation for a guideline regarding the ethical development and use of AI [5].

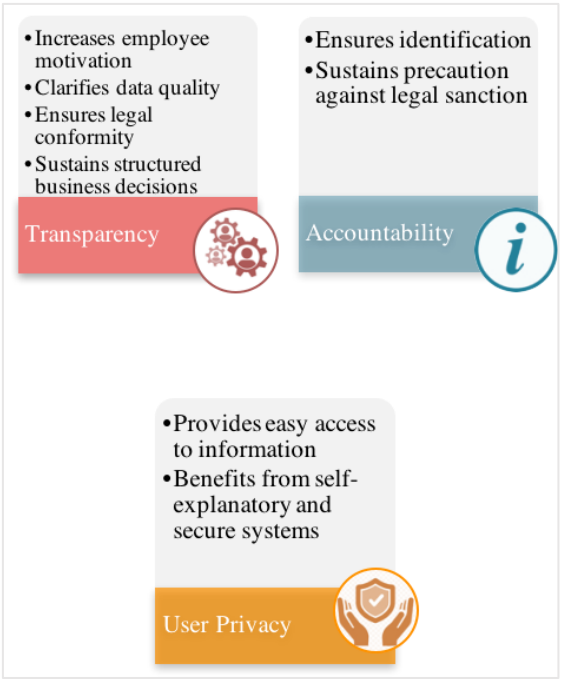

Figure 1. AI policy essentials

In response to these emerging concerns and new regulations, to build trust towards new technologies via sustainable and consistent systems, the companies are recommended to form an AI policy. Accordingly, within the scope of the paper, transparency, accountability and security aspects of AI implementations will be examined (Figure 1). Consequently, an AI policy will be recommended to be prepared to discuss the obstacles of the new technologies and ensure consistency in integration with the existing business processes. Although for each industry, it can be claimed that a specific AI policy should be formed, within the scope of the paper, the e-Commerce industry needs will be addressed.

To start with the first important issue, **transparency** is the quality of the system to support an understanding of the system behaviour, intentions and future goals [6]. The reason behind this claim is that trust depends on the granularity of explanations and on the transparency of the system [7]. Although the transparency of the system should be analysed separately for users inside and outside the organization, because of the limited scope of the paper, the more attention is given to the transparency determination for the users inside the organization. The transparency of the system may affect the employee perspective, understanding, and motivation towards the system. Therefore, the users need to be knowledgeable about the system to utilise it most efficiently.

To continue with **accountability**, when there is a mistake, a malfunction or a performance errors, which is caused by an AI technology's decisions and actions, it is difficult to determine who is responsible for and where the blame will be directed [7].

Therefore, while deciding on the architectural principles, it is claimed to be an essential aspect to sustain identification and legal compliance. Providing identification of the actions enables companies and their stakeholders to defend themselves against misbehaviour of the AI technology or deter it all together.

Lastly, the **security** and **user privacy** have been claimed to become complicated as the amount of collected data gets even higher when attempting to determine which data are personal and which are not [2]. While the discussion is still continuous, without a doubt, the questions related to user privacy and security has not been answered yet, and it is possible that the concerns may get more significant in the future as AI becomes a part of the daily life. Especially for the businesses, with the improvements in AI technologies, the tools, systems, and techniques become a part of the core processes. Therefore, the companies become vulnerable for any legal loophole or trust related issues.

For the proposed AI policy, transparency, accountability and security issues will be addressed and recommendations will be given for the e-commerce companies. In the next section, the recommendations for the e-commerce industry will be discussed.

3. THE RECOMMENDATIONS FOR FORMING AN AI POLICY

3.1 Transparency

As the first part of the AI policy, transparency issues and recommendations will be analysed according to the needs of the end users, who are working and using the AI technologies within the businesses. Apart from the previously discussed government policies, especially in business processes, the decisions and related actions should be precise as much as possible and be structured accordingly to prevent any misuse or actions against the regularity compliance. Therefore, in the following argument, the system **purpose**, the **process** and the **performance** (3Ps) are claimed to be important while constructing an AI policy.

3.1.1 System purpose

The first important aspect to pay attention is the communication with the end user about the reasoning behind a decision of the AI technology. Although the complexity of the algorithms may be too high, there are few successful implementation examples of sharing the system's purpose and reasoning with the end-user. For example, the logic behind the algorithm of Google's Gmail spam folder is provided through an alert box. When the user clicked on the query, which is 'why is this message in Spam?', the purpose and the reason are provided [4]. It can be recommended that a similar component can be used by e-Commerce companies. To sustain consistency and objectivity while the AI policy is formed, the details of such a component should be covered.

3.1.2 System process

While addressing the 'why should I trust?' question, the end users need to also broadly understand the process flow that an AI technology is following. At this point, the transparency of the system gains crucial importance. The awareness for transparency can be claimed to be sustained by providing the source data or services related to the user and his or her action. In other words, employees, managers and other possible end users should be provided the information on how data are collected and processed by the system. For that reason, the process and simplified algorithms should be revealed in a way that is understandable for the employees.

3.1.3 System performance

After realizing the reasoning of an AI technology and its process flow, the end user should be able to analyse the outcome. For example, a service company, Accenture, uses a 'Teach and Test' methodology to ensure that the AI systems are producing the right decision. The teaching is achieved by using the data which are gathered for training the machine learning algorithms. The testing, on the other hand, is claimed to be accomplished by comparing outcomes concerning key performance indicators. At this point, it can be recommended that the expected performance indicators should be formed so that transparency can be questioned by the employees, customers and other stakeholders. Following that, the purpose of the automation, the design basis and the previous performance metrics related to the user, i.e., the sales representative, should be included in the AI policy. However, as the technologies are emerging, the historical data may not be available. In this case, forecasted outcome expectations can be added to the policy.

In summary, the written or the visual representation of the 3Ps as well as the outcome expectations, which are based on historical data or estimation, can be included in the AI policy. Also, using alert boxes to provide easy access and assessing general technical knowledge of the employees are recommended to confirm the transparency. These actions aim to help the employees, managers and even the end users to understand the cause of a behaviour, the intention and the desired effect of the technology [12].

3.2 Accountability

The AI policy recommendations will continue with the discussion of the accountability issues. Specific attention will be given to the **identification** and the **legal compliance** of the systems. Accordingly, the combination of legal and technical attention while forming an AI policy is claimed to be necessary for embracing issues related to accountability.

It can be claimed that an e-personality to machines and robots can be given so that the difference between it and a corporate personality can be made for liability and damage issues. For example, Audi will be liable for an accident involving 2019 A8 model which uses an automated system powered by the AI technologies to drive [11]. Accordingly, to sustain identification, it is recommended to provide and keep track of the proof that parties have performed specific actions. Notably, it should be precise that who is being held accountable for what action to whom [3], [8].

Similarly, an AI implementation like a chatbot of an e-Commerce company should be considered as not just a tool but also a representative of the company. Depending on the case, the end users, hosts, service operators or content providers can all be accountable or be permitted to check the accountability.

To move on with the legal compliance, although the security incidents are stressed the need for accountability mechanisms, there are still loopholes. That implies a need for the partnership of **legal** and **technical** experts while building an AI policy. Accordingly, it can be recommended that e- Commerce companies should combine technical and legal aspects while designing the system architecture.

Overall, the identification and the legal compliance of the system are claimed to be sustained through designing and implementing

accountable AI systems for the e-commerce industry. To maintain identification, not only keeping track of the information regarding the performed action by the system but also determining who is the responsible person of that action are recommended to be addressed. For sustaining legal compliance, the e-commerce companies are recommended to combine legal and technical knowledge for forming their AI policy. In the next section, security and user privacy issues will be addressed.

3.3 Security and User Privacy

As the last part of the AI policy analysis, security and user privacy issues will be questioned. According to the discussion, it is recommended for companies to pay attention to provide **easy access** to the collected data, and design **protective** systems to ensure security. While forming and AI policy, the received data, the design decisions for sustaining security is recommended to be explicit.

While companies are looking for ways to monetize the collected data, the balance between sustaining confidentiality or using data for advertisement purposes can get lost. Therefore, companies are recommended to pay attention to facilitate easy access by the users to the personal data collected about them.

When the legal conformity issues are reviewed, not only the new Data Protection Regulation (DPR) but also the White House report from USA (2012) address the data protection issues created by the latest technologies. In the report, the Consumer Privacy Bill of Rights (FIPP) includes two crucial statements. The first one is about the right of the consumers to expect the context-related collection, usage, and discloser of the data which is provided by themselves. The second one points out the right to exercise control over what personal data can be collected and used by the companies.

Overall, companies should determine the **scope** of personal data which can be related to a person and design and implement the system in a way to enable the user to monitor and frame the boundaries of the private information domain. Also, companies should design and apply technology in the most secure way to protect user privacy. Respectively, it has been stated that the information regarding the collected data, the design of the system should be included in the AI policy.

4. CONCLUSION

The As the AI technologies are applied by more and more companies in every field of the business for different purposes, we proposed that it is necessary to form an AI policy to address issues about transparency, **accountability** and **user privacy**. Within the scope of this paper, the e-Commerce industry is chosen to explore industry implementations, issues, and future risks because of its intensive use of emerging AI technologies.

From the three main parts of an AI policy, firstly, transparency related issues are recommended to be clarified with the communication of the **purpose**, **process**, and **performance** (3Ps) details of the technology that is being used.

Along with sustaining transparency, determining the **ownership** and balancing the input of a **legal** and **technical** perspective while forming an AI policy are mentioned important for satisfying the need for an accountable technology.

Lastly, together with transparent and accountable implementation, sustaining user privacy and security is claimed to be inevitable for the success of the AI implementation and policy. To sustain user privacy and ensure security, the companies are recommended to provide **easy access** to the source information regarding the collected data and the mechanism behind the intelligence of the technology. In addition to providing information, it is also recommended to pay attention to designing **secure** and **self-explanatory** technologies from the start to ease sustaining privacy and security.

Although the AI policy should be framed differently for each industry and company, a general framework is proposed for the use of the companies. Also, to enhance the proposed AI strategy, different e-Commerce companies should be examined, and organizational, cultural and regulatory contexts should be considered which may differ for each company, country and the nature of the business. Nevertheless, in every case, while more attention is given to the exciting advancements of the technologies, the current issues and forecasted risks should not be overlooked.

5. REFERENCES

[1] Agrawal, A., Gans, J., & Goldfarb, A. (2017). What to expect from artificial intelligence. MIT Sloan Management Review.

[2] Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical Design in the Internet of Things. Science and Engineering Ethics, 24(3), 905-925

[3] Bechtold, S., & Perrig, A. (2014). Accountability in future internet architectures. Communications of the ACM, 57(9), 21-23.

[4] Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), Big Data & Society, 05 January 2016, Vol.3(1).

[5] Bunz, M., & Janciute, L. (2018). REVIEW OF POLICY OPTIONS. In Artificial Intelligence and the Internet of Things: UK Policy Opportunities and Challenges (pp. 14-17). London: University of Westminster Press. Retrieved from http://www.jstor.org/stable/j.ctv5vddtc.6

[6] Chen, Z., & Dubinsky, A. (2003). A conceptual model of perceived customer value in e-commerce: A preliminary investigation. Psychology and Marketing, 20(4), 323-347.

[7] Ewart J. de Visser, Richard Pak & Tyler H. Shaw (2018): From ‘automation' to ‘autonomy': the importance of trust repair in human- machine interaction, Ergonomics, DOI: 10.1080/00140139.2018.1457725

[8] Glass, A., McGuinness, D., & Wolverton, M. (2008) Toward establishing trust in adaptive agents. In Proceedings of the 13th international conference on intelligent user interfaces (pp. 227–236).

[9] Goodman, B. & Flaxman, S. 2017, "European Union Regulations on Algorithmic Decision Making and a "Right to Explanation", AI Magazine, vol. 38, no. 3, pp. 50-57.

[10] Griffith, E. (2017). It's time to take AI seriously. Fortune, 175(3), 51-51.

[11] Ju-Len, L. (2017, Aug 04). The age of autonomy. The Business Times, Retrieved from https://search-proquestcom.ezproxy.sussex.ac.uk/docview/1925864387?accountid= 14182

[12] Lee, J., & See, K. (2004). Trust in Automation: Designing for Appropriate Reliance. Human Factors: The Journal of Human Factors and Ergonomics Society, 46(1), 50-80.

[13] MacCarthy, M. 2017, "AI policy should be based on science, not science fiction", InfoWorld.com.

[14] Ng, A. (2016). What Artificial Intelligence can and can't do right now. Harvard Business Review. Retrieved from: https://hbr.org/2016/11/what-artificial-intelligence-can-and-cant-do-right-now

[15] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

[16] Ransbotham, S., Kiron, D., Gerbert, P., & Reeves, M. (2017). Reshaping Business With Artificial Intelligence: Closing the Gap Between Ambition and Action. MIT Sloan Management Review, 59(1).